Amendments to the Claims

This listing of claims will replace all prior version, and listings, of claims in the application:

Listing of Claims

1. (Previously presented) A network security system for permitting a trusted process using a firewall, the firewall protecting a corresponding network connection of a computer to a network by setting restrictions on information communicated between networks, comprising:

a port monitoring unit for extracting information about a server port being used by a network communication program;

an internal permitted program storage for storing a list of programs permitted to have server ports registered by the firewall, wherein the internal permitted program storage adds a program to the list by extracting information about the program for which communication is permitted by the firewall and registering the extracted information in the list;

a firewall flexible device for determining whether the network communication program is registered in the list of programs stored in the internal permitted program storage; and

an internal permitted port storage registering the extracted information about the server port if the firewall flexible device determines that the network communication program is registered in the list of programs stored in the internal permitted program storage;

wherein the firewall flexible device further determines whether a destination port of a packet of inbound traffic has been registered in the internal permitted port storage and blocks the packet of inbound traffic if the destination port has not been registered.

2. (Previously presented) The network security system as set forth in claim 1, wherein the information about the program, which is extracted and registered in the internal permitted program storage,

includes information about at least one of a program name, an entire path of the program, and a program hash value.

3. (Previously presented) The network security system as set forth in claim 1, wherein the information about the server port, which is registered in the internal permitted port storage, includes information about at least one of an entire path of the program, a protocol, and a port.

4. (Previously presented) A network security method of permitting a trusted process using a firewall, the firewall protecting a corresponding network connection of a computer to a network by setting restrictions on information communicated between networks, comprising:

storing in an internal permitted program storage a list of programs permitted to have server ports registered by the firewall;

extracting information about a server port being used by a network communication program;

determining whether the network communication program is registered in the list of programs stored in the internal permitted program storage;

registering the information about the extracted server port in an internal permitted port storage if the network communication program determined to be registered in the list of programs stored in the internal permitted program storage;

determining whether a destination port of a packet of inbound traffic has been registered in the internal permitted port storage; and

blocking the packet of inbound traffic if the destination port has not been registered.

5 - 7. (Canceled)

8. (Previously presented) The network security method as set forth in claim 4, wherein the information about the program includes

information about at least one of a program name, an entire path of the program, and a program hash value.

9. (Previously presented) The network security method as set forth in claim 4, wherein the information of the server port includes information about at least one of an entire path of the program, a protocol, and a port.

10. (Currently amended) A ~~computer-readable recording medium~~computer recordable device for performing a network security method using a firewall, the ~~medium~~device storing a program for executing the method, the method comprising:

storing in an internal permitted program storage a list of programs permitted to have server ports registered by the firewall;

extracting information about a server port being used by a network communication program;

determining whether the network communication program is registered in the list of programs stored in the internal permitted program storage;

registering the information about the extracted server port in an internal permitted port storage if the network communication program is determined to be registered in the list of programs stored in the internal permitted program storage;

determining whether a destination port of a packet of inbound traffic has been registered in the internal permitted port storage; and

blocking the packet of inbound traffic if the destination port has not been registered.

11. (Previously presented) The network security system as set forth in claim 1, wherein the firewall flexible device allows the packet of inbound traffic to bypass the firewall if the destination port has been registered.

12. (Previously presented) The network security method as set forth in claim 4, further comprising:

allowing the packet of inbound traffic to bypass the firewall if the destination port has been registered.

13. (New) The network security system as set forth in claim 1, wherein the internal permitted port storage registers the extracted information about the server port if the server port is determined to be opened.

14. (New) The network security system as set forth in claim 1, wherein the extracted information about the server port is deleted from the internal permitted port storage if the server port is determined to be closed.

15. (New) The network security method as set forth in claim 4, further including:

registering the extracted information about the sever port in the internal permitted port storage if the server port is determined to be opened.

16. (New) The network security method as set forth in claim 4, further including:

deleting the extracted information about the sever port from the internal permitted port storage if the server port is determined to be closed.

17. (New) The computer recordable device as set forth in claim 10, wherein the method further including:

registering the extracted information about the sever port in the internal permitted port storage if the server port is determined to be opened.

18. (New) The computer recordable device as set forth in claim 10, wherein the method further including:

deleting the extracted information about the sever port from the internal permitted port storage if the server port is determined to be closed.